AMENDMENTS TO THE CLAIMS

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

Claim 1. (*Currently Amended*) A method of making information contents of memory cells of a volatile semiconductor memory irretrievable, said method comprising:

generating a digital pattern;

~~overwriting~~ writing the information contents ~~of~~ in the memory cells ~~with a pattern based upon the digital pattern a first time~~ at a first rate during normal processing before tampering is detected; and

overwriting the information contents ~~of~~ in the memory cells with a pattern based upon the digital pattern at least ~~a second~~ two times ~~time~~ at a second rate greater than the first rate after detecting tampering.

Claim 2. (*Currently Amended*) A method according to claim 1, in which said ~~digital~~ pattern overwrites said information contents alternately with its complementary pattern.

Claim 3. (*Currently Amended*) A method according to claim 1, in which said ~~digital~~ pattern is a predefined digital pattern comprising both zeros and ones.

Claim 4. (*Previously presented*) A method according to claim 3, in which a ratio of the number of zeros and the number of ones in said predefined digital pattern is about one.

Claim 5. (*Original*) A method according to claim 4, in which said ratio differs less than thirty percent from one.

Claim 6 (*Original)* A method according to claim 4, in which said ratio is one.

Claim 7. (*Original*) A method according to claim 1, in which said digital pattern is a random pattern.

Claim 8. (*Currently Amended*) A device comprising a cryptographic chip and a tampering signal generating device for generating a tampering signal upon detection of tampering with the chip, said cryptographic chip comprising a volatile semiconductor memory having a plurality of memory cells, a control device for placing a cryptographic key in memory cells of said volatile semiconductor memory, a pattern generating device for generating a digital pattern, an address generating device for generating addresses of said memory cells, said pattern generating device and said address generating device being connectable to said volatile semiconductor memory, said tampering signal generating device being connected to said pattern generating device and said address generating device, said pattern generating device and said address generating device being adapted for ~~in response to a said tampering signal~~ being connected to said volatile semiconductor memory and overwriting contents ~~of~~ in said memory cells with a pattern based upon said digital pattern for at

least two times in response to said tampering signal, in which said cryptographic chip comprises first connecting means connecting an output of said pattern generating device to a data input of said volatile semiconductor memory, second connecting means for connecting said address generating device to an address input of said volatile semiconductor memory and a clock generator for generating clock signals for said pattern generating device and said address generating device, and comprising a digital processor adapted to successively address addresses of said memory cells at a first rate during normal operation before tampering is detected, said clock generating device and said address generating device being adapted when operating together to successively address addresses of said memory cells at a second rate greater than said first rate in response to said tampering signal.

Claim 9 (*Canceled*)

Claim 10. (*Original*) A device according to claim 8, in which said digital pattern is a predefined digital pattern comprising both zeros and ones.

Claim 11. (*Original*) A device according to claim 8, in which said digital pattern alternately is said digital pattern and a complementary pattern of said digital pattern.

Claim 12. (*Previously presented*) A device according to claim 8, said device being adapted to have a power down state in which no main power is supplied to said device, said device comprising a battery back up power supply, said pattern generating device, said clock generator and said address generating device being permanently connected to said back up battery power supply.

Claim 13 (*Canceled*)

Claim 14. (*Previously presented*) A device according to claim 8, in which said second rate is substantially greater than said first rate.

Claim 15. (*Previously presented*) A device according to claim 8, in which said second rate is such that all addresses of said memory cells may be addressed at least three times within 1 millisecond.

Claim 16. (*Currently Amended*) A device comprising a cryptographic chip and a tampering signal generating device for generating a tampering signal in response to tampering with the chip, said cryptographic chip comprising a volatile semiconductor memory having a plurality of memory cells, a control device for placing a cryptographic key in memory cells of said volatile semiconductor memory, a pattern generating device for generating a digital pattern, an address generating device for generating addresses of said memory cells, said pattern generating device and said address generating device being connectable to said volatile semiconductor memory, said tampering signal generating device being connected to said pattern generating device and said address generating device, a processor adapted to write contents in said memory cells at a first rate during normal

processing, said pattern generating device and said address generating device being adapted for connection to said volatile semiconductor memory and for ~~for in response to a said tampering signal being connected to said volatile semiconductor memory and overwriting contents of said memory cells with a pattern based upon said digital pattern for a first time at a first rate, and~~ overwriting contents ~~of~~ in said memory cells with pattern based on said digital pattern for ~~a second time~~ at least two times at a second rate greater than the first rate in response to said tampering signal.

Claim 17. (*Previously presented*) A device according to claim 16, in which said digital pattern is a predefined digital pattern comprising both zeros and ones.

Claim 18. (*Previously presented*) A device according to claim 16, in which said digital pattern alternately is said digital pattern and a complementary pattern of said digital pattern.

Claim 19. (*Previously presented*) A device according to claim 16, said device being adapted to have a power down state in which no main power is supplied to said device, said device comprising a battery back up power supply, said pattern generating device, said clock generator and said address generating device being permanently connected to said back up battery power supply.

Claim 20. (*Previously presented*) A device according to claim 16, in which said second rate is substantially greater than said first rate.

Claim 21. (*Previously presented*) A device according to claim 16, in which said second rate is such that all addresses of said memory cells may be addressed at least three times within 1 millisecond.

Claim 22. (*New*) A method according to claim 1, further comprising:

generating the first rate using a processor; and

generating the second rate using an oscillator separate from the processor.